# ESPIONAGEM & FILOSOFIA
# SPY & PHILOSOPHY

***SILVA JR., Nelmon J.***[1]

**RESUMO:** Frente à ameaça de espionagem cibernética dos EUA no Brasil, faz-se necessária mudança institucional para o resguardo de nossa soberania.
**PALAVRAS-CHAVE:** Cibercrime. Cientistas. Legislação. Educação. Liberdade.

**SUMMARY:** Faced with the threat of cyber espionage the U.S.A. In Brazil, it is necessary institutional change to guard our sovereignty.
**KEYWORDS:** Cybercrime. Scientists. Legislation. Education. Freedom.

*No domingo (6), o jornal "o Globo" informou que a Agência de Segurança Nacional dos Estados Unidos (NSA, na sigla em inglês) espionou milhões de e-mails e ligações telefônicas de brasileiros. Reportagem publicada também pelo "O Globo" nesta segunda aponta que até 2002 funcionou em Brasília uma das estações de espionagem nas quais agentes da NSA trabalharam em conjunto com a Agência Central de Inteligência (CIA) dos Estados Unidos.*[2]

*O ministro Antônio Patriota informou que o governo solicitará esclarecimento a Washington e ao embaixador norte-americano sobre o caso. "O governo brasileiro promoverá no âmbito da União Internacional de Telecomunicações (UIT) em Genebra, o aperfeiçoamento de regras multilaterais sobre segurança das telecomunicações. Além disso, o Brasil lançará nas Nações Unidas iniciativas com o objetivo de proibir abusos e impedir a invasão da privacidade dos usuários das redes", disse.*[3]

*Ideli deu a declaração ao comentar a denúncia de que o Brasil é um dos alvos de espionagem dos Estados Unidos. Para a ministra, a soberania do país e a privacidade dos brasileiros estão "em*

---

1 **CIENTISTA E ESTUDIOSO DO DIREITO (PROCESSUAL) PENAL - CV Lattes:** http://lattes.cnpq.br/7382506870445908
1.MANTENEDOR DOS BLOGS CIENTÍFICOS:
http://ensaiosjuridicos.wordpress.com - http://propriedadeindustriallivre.wordpress.com
2. CIENTISTA COLABORADOR: Universidade Federal de Santa Catarina – UFSC (Portal de e-governo) http://www.egov.ufsc.br/portal/ - Glocal University Network http://www.glocaluniversitynetwork.eu/ (ITA)
3. MEMBRO: Centro de Estudios de Justicia de las Américas – CEJA (AL); Instituto de Criminologia e Política Criminal – ICPC; Associação Brasileira dos Advogados Criminalistas – ABRACRIM; Associação dos Advogados Criminalistas do Paraná – APACRIMI; International Criminal Law – ICL (EUA); National Association of Criminal Defense Lawyers (EUA).
4. MEMBRO FUNDADOR: Associação Industrial e Comercial de Fogos de Artifícios do Paraná/PR; e AINCOFAPAR (Conselheiro Jurídico), Associação Bragantina de Poetas e Escritores
5. COLABORADOR DAS SEGUINTES MÍDIAS: www.arcos.org.br - www.conteudojuridico.com.br - http://artigocientifico.uol.com.br - http://www.academia.edu/ - http://pt.scribd.com/ - http://www.academicoo.com/
6. AUTOR DOS SEGUINTES LIVROS CIENTÍFICOS: Fogos de Artifício e a Lei Penal; Coletâneas; e Propriedade Intelectual Livre.
7. AUTOR DOS SEGUINTES LIVROS LITERÁRIOS: Nofretete, Copo Trincado, e Valhala.

2 Texto disponível em: http://g1.globo.com/politica/noticia/2013/07/senadores-querem-explicacoes-sobre-espionagem-dos-eua-no-brasil.html. Acesso em 09.07.2013.

3 Texto disponível em: http://g1.globo.com/politica/noticia/2013/07/senadores-querem-explicacoes-sobre-espionagem-dos-eua-no-brasil.html. Acesso em 09.07.2013.

*xeque". [...] disse que a espionagem é "inadmissível" e que o governo espera uma "movimentação ágil, efetiva e urgente" do Congresso Nacional para a aprovação do Projeto de Lei enviado pelo governo em 2011 e que estabelece direitos e deveres de usuários, governo e empresas no uso da rede.*[4]

*Eu não tenho dúvida nenhuma [de que o governo dos EUA monitorou brasileiros]. Até o Parlamento Europeu foi monitorado, você acha que nós não fomos? Agora, as circunstâncias em que isso se deu, a forma exata e a data, isso temos que verificar", disse Bernardo ao deixar a sede do Ministério das Comunicações no início da tarde desta segunda.*[5]

Lendo estas preocupantes notícias, forçosamente relembrei de artigo de minha autoria (31.05.2013) :

*Após a Guerra Fria o terrorismo tornou-se mais evidente (perceptível) à Nações, sendo que suas formas operacionais e objetivas também adequaram-se frente à realidade cibernética global. Hoje não são necessários tantos suicidas dogmáticos para concretizar o intento criminoso terrorista, como no quinquênio passado. Os ataques às ciber-redes dos Estados aterrorizados por esses grupos estão cada dia mais comuns e sofisticados, sendo tal fenômeno globalmente conhecido por ciberterror(ismo). O combate ao ciberterror é (talvez) nosso maior desafio enquanto sociedade pré-globalizada.*

*A moeda forte e respeitável produção científica, já não representam mais estabilidade à maioria das Nações, pois esses valores (meramente conceituais) não a(s) protege(m) contra eventuais ataques terroristas, sublinhe-se, facilitados estrategicamente pela rede cibernética que sustenta estruturalmente nossos Estados. Pois bem, os países mais desenvolvidos (como no passado eram chamados) estão tão (ou mais) vulneráveis a ataques terroristas quanto àqueles menos desenvolvidos. O pânico e insegurança violentamente impostos pelo Regime do Terror ao mundo globalizado, colocam em xeque aquele conceito pretérito de soberania, que simplesmente conceituada, traduz-se no poder ou autoridade absoluta do Estado sobre seu povo e território.*[6]

Em sequencia, relembrei de meu recente artigo (25.06.2013), onde questionava o que o seu País tem feito em relação ao combate do cibercrime e do ciberterrorismo; e quanto à seguridade cibernética de seu povo:

*Segundo dados da Asian School of Cyber Laws*[7]*, gasta-se atualmente no mundo cerca de US$ 45.000.000,00, no combate ao crime cibernético e seus efeitos, razão pela qual inúmeros países tem-se antecipado na cruzada contra (grupo(s) terroristas cibernéticos.*

*Ainda, para o autor existem sete nações que possuem uma política de guerra cibernética, a saber: República Popular da China, Índia, Irã, Coreia do Norte, Paquistão, Rússia e Estados Unidos da América*[8]*. Sou obrigado a*

4 Texto disponível em: http://g1.globo.com/politica/noticia/2013/07/ministra-quer-marco-civil-da-internet-e-diz-que-soberania-esta-em-xeque.html. Acesso em 09.07.2013.

5 Texto disponível em: http://g1.globo.com/politica/noticia/2013/07/ministro-diz-nao-ter-duvida-de-que-eua-espionaram-brasileiros.html. Acesso em 09.07.2013.

6 Texto disponível em: http://ensaiosjuridicos.wordpress.com/2013/06/02/ideologia-e-soberania-nelmon-j-silva-jr/. Acesso em 09.07.2013.

7 Texto disponível em: http://www.facebook.com/asianschoolofcyberlaws?fref=ts. Acesso em 25.06.2013.

8 *Óp. cit,* p. 16 *usque* 20.

*discordar dos dados citados pelo autor, ao analisar o sítio virtual da International Telecomunication Union – ITU, em especial daqueles constantes da Global Cybersecurity Agenda – GCA.*[9]

*Percebam que nações, como à exemplo da Índia, investem na formação (gratuita) de profissionais de segurança cibernética, pois segundo suas fontes governamentais, até 2015, serão necessários mais de 4.700 profissionais nesta área.*[10]-[11]

Para bem dimensionar a extensão do problema em vértice, faz-se necessário citar:

*existem mais de setenta formas de agressões cibernéticas: Anonymizer; ARP cache poisoning; Backdoor; Backscatter; The Blues- Bluebugging, Bluejacking and Bluesnarfing; Buffer overflow; Bullying in Cyberspace; Click fraud; Computer trespass; Cookie Manipulation; Copyright infringement; Crap-flooding; Cyber Stalking; Cyber Terrorism; Cyber Warfare; Data Diddling; Data Leakage; Defamation; DOS / DDOS; DNS poisoning; Easter Eggs; Email Spoofing; Encryption use by terrorists; eShoplifting; Financial Crimes; Fire Sale; Fire Walking; Footprinting; Fraud; Online Gambling; Google based hacking; Griefers; Hactivism; Hijacking; Identity Fraud; Impersonation; Joe – Job; Key stroke Logging; Logic Bomb; Lottery Scam; Mail Bombing; Malware; Nigerian 419 Fraud Scheme; Packet Sniffing; Phishing & Spoofing attacks; Piggy backing; Piracy of Software; Pod Slurping; Poisoning the Source; Pornography; robots.txt file; Port scanning; Rootkits; Salami Theft; Sale of Illegal Articles; Scavenging; Smishing; Social Engineering; Spambot; SQL Injection; Stealware; Time Bomb; Trojan; URL Manipulation; Virus Attack; Web defacement; Vishing; Wire – Tapping; Worm; XSS Attack; Y2K; Zero Day Attack; Zeus; e Zombie.*[12]_[13]

Dito isto, passo a desenvolver meu raciocínio, como faziam os socráticos, através da maiêutica[14]. 1. Nossos Oficiais das Forças Armadas, Parlamentares e Líderes do Executivo e Legislativo possuem conhecimento técnico-científico suficiente para bem atuarem no combate e prevenção ao cibercrime e ciberterrorismo? 2. Seria mais prudente, ao invés de aprovar(em)-se lei(s) às pressas, convocar estudiosos e cientistas desta vasta e complexa matéria, para elaborarem um projeto de lei, definindo condutas delitivas e respectivas sanções legais? 3. Estratégias cibernéticas antiterroristas são necessárias ao reguardo da nossa Soberania? 4. Exemplos pedagógicos como os hodiernamente adotados pela Índia e China, devem ser priorizados pelo Governo Federal?

---

9 http://www.itu.int/osg/csd/cybersecurity/gca/ - acesso em 25.06.2013.

10 http://m.economictimes.com/news/news-by-industry/jobs/around-4-7-lakh-cyber-security-professionals-needed-by-2015-milind-deora/articleshow/17430201.cms. Acesso em 25.06.2013.

11 Texto disponível em:http://ensaiosjuridicos.wordpress.com/2013/06/25/ciber-terror-ciber-guerra-nelmon-j-silva-jr/. Acesso em 09.07.2013.

12 SHAH. Aaushi,. RAVI. Srinidhi,. ***A to Z of Cyber Crime.*** Asian School of Cyber Laws. 2013. Livro disponível em: http://ensaiosjuridicos.files.wordpress.com/2013/06/122592201-cybercrime.pdf

13 Texto disponível em:http://ensaiosjuridicos.wordpress.com/2013/06/25/ciber-terror-ciber-guerra-nelmon-j-silva-jr/. Acesso em 09.07.2013.

14 A maiêutica é um método de ensino socrático, no qual o professor se utiliza de perguntas que se multiplicam para levar o aluno a responder às próprias questões.

Comungo da ideia de que *quando um país está atolado na corrupção, costuma haver alianças entre organizações criminosas com força política e instituições encarregadas de proteger a ordem pública. Os baixos salários do serviço público são um fator desencadeador. As pessoas sofrem com a corrupção e sentem que os criminosos estão agindo com impunidade*.[15]

Por derradeiro, cito a - aplicável - lição deixada por Johann Goethe: *ninguém é mais escravo do que aquele que se julga livre sem o ser;* portanto, assim sustento as ideias acima trazidas, em forma de - necessário - questionamento (nacional).

15 PAGET. François, ***Cibercrime e hacktivismo.*** McAfee Labs™. 2010. p. 19. Livro disponível em: http://ensaiosjuridicos.files.wordpress.com/2013/06/79513582-mcafee-cybercrime-hactivism.pdf